ЗАНЯТТЯ № 2

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ НА ОСНОВІ ГРУПУВАННЯ ПОРТІВ І ТРАНКОВОГО ПРОТОКОЛУ 802.1Q У МЕРЕЖАХ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження технології VLAN на основі групування портів і транкового протоколу 802.1Q на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи VLAN, побудованих на базі комутаторів Cisco із застосуванням агрегованих транкових каналів (EtherChannel); дослідити процеси розмежування широкомовних доменів, ізоляції трафіку різних VLAN та забезпечення централізованого керування мережею через виділену VLAN управління; навчитися налаштовувати захищений SSH-доступ до комутаторів з VLAN управління.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Керовані комутатори Cisco серії Catalyst 2960 (моделі WS-C2960-24TT-L або WS-C2960-48TT-L або WS-C2960S-F24TS-L або WS-C3560-24TS) – 3 шт.
2. Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 2 шт.
3. Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
4. Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 8 шт.
5. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочій станції.

Схема підключення

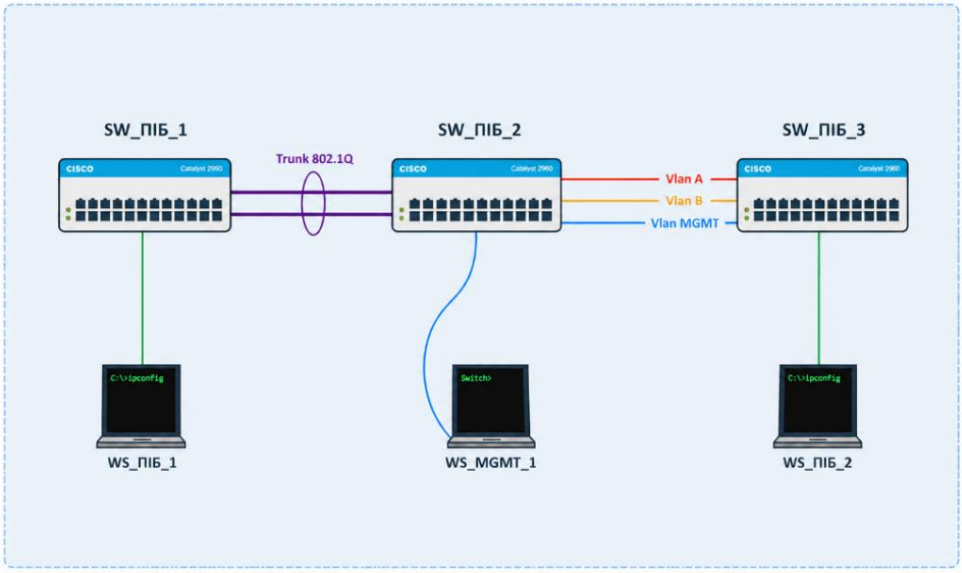

Рис. 2.1. Схема мережі, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва комутатора має бути у форматі SW_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевIРити наявність консольних та Ethernet-кабелів.
2. Створити мережу відповідно до схеми на рис. 2.1. Під час побудови звернути увагу на вибIР типу кабелів та порядок підключення.
3. Провести налагодження іменування всіх 3 пристроїв (SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3) та встановити захищений пароль привілейованого режиму (**enable secret**).
4. Розробити схему IP-адресації пристроїв мережі згідно з варіантом (табл. 2.4). Заповнити таблицю адресації 2.1.

Таблиця 2.1.

Параметри адресації мережі

Мережа/Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс
VLAN даних A	–	–			
VLAN даних B	–	–			
VLAN керування	–	–			
SW1	Vlan				
SW2	Vlan				
SW3	Vlan				
WS1	NIC				
WS2	NIC				

5. Визначити номери VLAN згідно з варіантом (табл. 2.3). Заповнити таблицю 2.2 параметрів VLAN.

Таблиця 2.2.

Параметри VLAN мережі

Призначення VLAN	Назва VLAN	Номер VLAN
VLAN даних A		
VLAN даних B		
VLAN керування		

6. Виконати налаштування **VLAN** на всіх трьох комутаторах:

- На всіх трьох комутаторах (SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3) створити VLAN згідно з табл. 2.3, задати їм назви.
- Між комутаторами SW_ПІБ_1 та SW_ПІБ_2 налаштувати агрегований канал **EtherChannel** на двох фізичних Ethernet-інтерфейсах (режим згідно з табл. 2.3).
- Між комутаторами SW_ПІБ_1 та SW_ПІБ_2 налаштувати транковий канал який дозволятиме проходження VLAN даних A, B та VLAN управління. Налаштувати **Native VLAN** як VLAN за варіантом табл. 2.3. Вимкнути **DTP** командою **switchport nonegotiate**.
- Між комутаторами SW_ПІБ_2 та SW_ПІБ_3 налаштувати групування портів (окремий канал для кожної Vlan).

- На всіх трьох комутаторах налаштувати різні порти доступу для WS_ПІБ_1 та WS_ПІБ_2 для різних VLAN.

7. Налаштувати VLAN управління на всіх трьох комутаторах, призначити IP-адреси відповідно до табл. 2.1.

8. Налаштувати захищений SSH-доступ на всіх трьох комутаторах:

- Задати доменне ім'я (**ip domain-name**);
- Створити 2 користувачів (**Admin** та **User**) з рівнями привілеїв 15 та 1;
- Згенерувати RSA-ключі (**crypto key generate rsa modulus 2048**);
- Активувати SSHv2 (**ip ssh version 2**);
- Налаштувати лінії VTY на прийом виключно SSH-з'єднань (**transport input ssh**).

9. Налаштувати параметри IP-адресації на робочих станціях WS_ПІБ_1 та WS_ПІБ_2 відповідно до табл. 2.1 для перевІРки зв’язку спочатку однакових VLAN а потім різних.

10. ПеревІРити наявність зв'язку в мережі:

- Командою **ping** підтвердити доступність між WS_ПІБ_1 та WS_ПІБ_2 з однієї VLAN.
- Командою **ping** підтвердити відсутність зв’язку між WS_ПІБ_1 та WS_ПІБ_2 з різних VLAN.
- Командою ping перевІРити доступність усіх трьох комутаторів з WS_ПІБ_1 через VLAN керування.
- Підключитися до кожного комутатора по SSH з WS_ПІБ_1 або WS_ПІБ_2 та переконатися у правильності налаштувань доступу через VLAN керування.

11. Дослідити результати налаштувань за допомогою команд: **show vlan brief**, **show vlan**, **show interfaces switchport**, **show interfaces trunk**, **show interfaces port-channel switchport**, **show etherchannel summary**, **show dtp**, **show ip ssh**, **show users**, **show running-config**.

12. Дослідити відмовостійкість агрегованого транкового каналу: відключити один із фізичних інтерфейсів EtherChannel командою **shutdown** та перевІРити збереження зв’язку між VLAN командою **ping**. Поновити інтерфейс командою **no shutdown**.

13. Вивести та проаналізувати файли конфігурацій усіх трьох комутаторів (**show running-config**).

14. У випадку виявлення помилок у налагодженнях – визначити причину та усунути їх.

15. Продемонструвати виконану роботу керівнику практики та оформити звіт.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти.

Таблиця 2.3.

Параметри налаштування VLAN та транкового каналу

№ в-та	VLAN A	VLAN B	VLAN MGMT	SW1–SW2 (EtherChannel)	SW2–SW3 (trunk)	Native VLAN
1	10	20	100	on / on	trunk/on	A
2	11	21	200	desirable / desirable	dynamic desirable	B
3	12	22	300	desirable / auto	trunk/on	A
4	13	23	400	auto / desirable	dynamic desirable	B
5	14	24	500	active / active	trunk/on	A
6	15	25	600	active / passive	trunk/on	B
7	16	26	700	passive / active	dynamic desirable	A
8	17	27	800	on / on	trunk/on	B
9	18	28	900	desirable / desirable	dynamic desirable	A
10	19	29	110	desirable / auto	trunk/on	B
11	30	40	120	auto / desirable	dynamic desirable	A
12	31	41	130	active / active	trunk/on	B
13	32	42	140	active / passive	dynamic desirable	A
14	33	43	150	passive / active	trunk/on	B
15	34	44	160	on / on	dynamic desirable	A
16	35	45	170	desirable / desirable	trunk/on	B
17	36	46	180	desirable / auto	dynamic desirable	A
18	37	47	190	auto / desirable	trunk/on	B
19	38	48	210	active / active	dynamic desirable	A
20	39	49	220	active / passive	trunk/on	B

Таблиця 2.4.

Параметри IP-адресації мережі

№ в-та	IP VLAN A	Prefix	IP VLAN B	Prefix	IP VLAN MGMT	Prefix	IP-адреса шлюзу за замовчуванням/
1	191.C.S.0	/24	192.C.S.0	/25	172.C.S.0	/27	Перша IP-адреса діапазону
2	192.C.S.0	/25	193.C.S.0	/26	172.C.S.0	/28	Остання IP-адреса діапазону
3	193.C.S.0	/26	194.C.S.0	/27	172.C.S.0	/29	Перша IP-адреса діапазону
4	194.C.S.0	/27	195.C.S.0	/28	172.C.S.0	/27	Остання IP-адреса діапазону
5	195.C.S.0	/28	196.C.S.0	/24	172.C.S.0	/28	Перша IP-адреса діапазону
6	196.C.S.0	/24	197.C.S.0	/25	172.C.S.0	/29	Остання IP-адреса діапазону
7	197.C.S.0	/25	198.C.S.0	/26	172.C.S.0	/27	Перша IP-адреса діапазону
8	198.C.S.0	/26	199.C.S.0	/27	172.C.S.0	/28	Остання IP-адреса діапазону
9	199.C.S.0	/27	200.C.S.0	/28	172.C.S.0	/27	Перша IP-адреса діапазону
10	200.C.S.0	/28	201.C.S.0	/24	172.C.S.0	/29	Остання IP-адреса діапазону
11	201.C.S.0	/24	202.C.S.0	/25	172.C.S.0	/27	Перша IP-адреса діапазону
12	202.C.S.0	/25	203.C.S.0	/26	172.C.S.0	/28	Остання IP-адреса діапазону
13	203.C.S.0	/26	204.C.S.0	/27	172.C.S.0	/29	Перша IP-адреса діапазону
14	204.C.S.0	/27	205.C.S.0	/28	172.C.S.0	/27	Остання IP-адреса діапазону
15	205.C.S.0	/28	206.C.S.0	/24	172.C.S.0	/28	Перша IP-адреса діапазону
16	206.C.S.0	/24	207.C.S.0	/25	172.C.S.0	/29	Остання IP-адреса діапазону
17	207.C.S.0	/25	208.C.S.0	/26	172.C.S.0	/27	Перша IP-адреса діапазону
18	208.C.S.0	/26	209.C.S.0	/27	172.C.S.0	/28	Остання IP-адреса діапазону
19	209.C.S.0	/27	210.C.S.0	/28	172.C.S.0	/29	Перша IP-адреса діапазону
20	210.C.S.0	/28	191.C.S.0	/24	172.C.S.0	/27	Остання IP-адреса діапазону

***Примітка*: C** (class) – номер аудиторії: для ауд. **107 – 71**, для ауд. **107a – 72, S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.
2. Короткі теоретичні відомості (за власним конспектом, обсягом 2–3 сторінки) з таких питань: концепція та призначення VLAN, метод групування портів, стандарт IEEE 802.1Q та транкові канали, формат кадру 802.1Q, протокол DTP, SVI-інтерфейс, VLAN управління, протокол SSH (порівняння з Telnet), налаштування SSH на Cisco.
3. Перелік використаного обладнання та програмного забезпечення.
4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв (SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3) та інтерфейсів, через які виконано з'єднання.
5. Розроблену схему IP-адресації у вигляді табл. 2.1 та параметри VLAN у вигляді табл. 2.2 з конкретними значеннями та розрахунками.
6. Лістинги команд (або скріншоти термінального вікна) з результатами виконання для кожного підзавдання 3–13, а саме:
   - налаштування VLAN на кожному комутаторі;
   - налаштування агрегованого каналу EtherChannel між SW_ПІБ_1 та SW_ПІБ_2;
   - налаштування транкового каналу між SW_ПІБ_1 та SW_ПІБ_2;
   - налаштування IP адрес та шлюзу за замовчуванням на всіх комутаторах;
   - налаштування SSH на всіх трьох комутаторах;
   - налаштування IP-адресації робочих станцій;
   - результати перевІРки зв'язку (**ping** між WS, **ping** до комутаторів);
   - доступ по SSH до кожного комутатора;
   - вивід команд діагностики: **show vlan brief**, **show interfaces trunk**, **show interfaces switchport**, **show etherchannel summary**, **show dtp**, **show ip ssh, show users**;
   - результати дослідження відмовостійкості **EtherChannel**.
7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.
8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Загальні відомості про VLAN

VLAN (Virtual Local Area Network, віртуальна локальна мережа) – логічна група вузлів комутованої мережі, що взаємодіють між собою так, ніби вони підключені до одного фізичного комутатора, незалежно від їхнього реального фізичного розташування. Технологія VLAN стандартизована у документі IEEE 802.1Q.

Традиційна комутована мережа без VLAN є єдиним широкомовним доменом: кожен широкомовний кадр (ARP-запит, DHCP-запит тощо) отримує і обробляє кожен хост мережі. Зі збільшенням кількості вузлів це призводить до

зростання широкомовного трафіку та деградації продуктивності. VLAN вирішує цю проблему шляхом поділу єдиного фізичного комутатора на кілька ізольованих логічних сегментів – широкомовних доменів.

Основні переваги використання VLAN:

- **Зменшення широкомовних доменів** – широкомовний трафік обмежений межами VLAN і не поширюється на інші VLAN;
- **Підвищення безпеки** – вузли різних VLAN не можуть безпосередньо взаємодіяти між собою без участі маршрутизатора або L3-комутатора;
- **Гнучка логічна структура** – адміністратор може об'єднувати вузли у логічні групи незалежно від їхнього фізичного розташування;
- **Спрощення адміністрування** – переміщення вузла між VLAN виконується засобами конфігурування комутатора без фізичного перепідключення;
- **Якість обслуговування (QoS)** – різним VLAN можна призначати різні пріоритети передачі трафіку.

Методи ідентифікації VLAN

Існують різні методи визначення приналежності вузла або кадру до тієї чи іншої VLAN:

- **Групування портів (port-based VLAN)** – найпоширеніший метод. Кожному фізичному порту комутатора призначається певний ідентифікатор VLAN (VID). Кадри, що надходять через цей порт, вважаються такими, що належать відповідній VLAN. Метод не вимагає модифікації кінцевих пристроїв.
- **VLAN на основі MAC-адрес** – VLAN визначається на основі MAC-адреси відправника кадру. Таблиця відповідності MAC-адрес та VLAN зберігається в спеціальному сервері VMPS (VLAN Membership Policy Server). Метод гнучкий, але складніший в адмініструванні.
- **VLAN на основі протоколу** – VLAN визначається за типом мережного протоколу (наприклад, IP, IPX, AppleTalk). Зазвичай реалізується у комутаторах рівня 3.
- **VLAN на основі аутентифікації (802.1X)** – VLAN призначається динамічно після успішної аутентифікації користувача за протоколом 802.1X.

Призначення та суть транкових каналів

Порт доступу (access port) підключає кінцевий пристрій до одної конкретної VLAN та передає нетеговані кадри. Проте в комутованій мережі з кількома VLAN постає завдання передачі трафіку різних VLAN між комутаторами через один фізичний канал. Для цього використовуються транкові канали (trunk links).

Транковий канал – це канал між двома комутаторами (або між комутатором і маршрутизатором), через який передаються кадри, що належать кільком різним VLAN. Щоб отримувач знав, до якої VLAN належить кожен кадр, застосовується механізм тегування.

Формат кадру IEEE 802.1Q

Стандарт IEEE 802.1Q визначає механізм тегування кадрів Ethernet для передачі по транковому каналу. Відповідно до цього стандарту, до стандартного кадру Ethernet між полями Source MAC та Type/Length вставляється 4-байтовий тег 802.1Q (VLAN-тег).

Структура тегу 802.1Q (4 байти):

- **TPID (Tag Protocol Identifier, 2 байти)** – ідентифікатор протоколу тегування, завжди дорівнює 0x8100 для 802.1Q;
- **TCI (Tag Control Information, 2 байти)** – поле управління тегом, що включає:
- **PCP (Priority Code Point, 3 біти)** – пріоритет кадру за стандартом IEEE 802.1p (0–7);
- **DEI (Drop Eligible Indicator, 1 біт)** – індикатор дозволу на відкидання кадру при перевантаженні мережі;
- **VID (VLAN Identifier, 12 біт)** – ідентифікатор VLAN, діапазон значень 0–4095; для мереж Ethernet активно використовується діапазон 2–1001.

Таким чином, 12-бітове поле VID дозволяє ідентифікувати до 4096 різних VLAN (0–4095), з яких VLAN 0 та VLAN 4095 зарезервовані, а VLAN 1 є VLAN за замовчуванням на обладнанні Cisco.

Порівняльна таблиця форматів кадру Ethernet та 802.1Q наведена в табл. 2.5.

Таблиця 2.5.

Порівняння форматів кадру стандартного Ethernet та IEEE 802.1Q

Поле	Звичайний Ethernet	802.1Q кадр	РозмIP	Значення/Діапазон
Destination MAC	+	+	6 байт	MAC-адреса отримувача
Source MAC	+	+	6 байт	MAC-адреса відправника
802.1Q Tag (TPID+TCI)	–	+	4 байти	0x8100 + PCP+DEI+VID
Ethertype / Length	+	+	2 байти	Тип протоколу
Payload (Data)	+	+	46–1500 байт	Дані
FCS (CRC)	+	+	4 байти	Контрольна сума

Протокол тегування ISL (Inter-Switch Link)

ISL (Inter-Switch Link) – фIPмовий протокол Cisco для тегування кадрів у trunk-каналах, розроблений до появи стандарту IEEE 802.1Q. На відміну від 802.1Q, ISL не вставляє тег всередину кадру, а повністю інкапсулює (обгортає) оригінальний Ethernet-кадр у новий ISL-заголовок (26 байт) та трейлер (4 байти). Це збільшує максимальний розмIP кадру з 1518 до 1548 байт.

Ключові відмінності ISL від IEEE 802.1Q наведені у табл. 2.6.

Таблиця 2.6.

Порівняння ISL та IEEE 802.1Q

Характеристика	ISL	IEEE 802.1Q
Розробник	Cisco (фІРмовий)	IEEE (відкритий стандарт)
Метод тегування	Повна інкапсуляція кадру	Вставка 4-байтового тегу
РозмІР накладних витрат	30 байт (26 + 4)	4 байти
Native VLAN	Не підтримується	Підтримується
Максимум VLAN	1000	4094
Підтримка на 2960/3650/3850	Відсутня	Є
Підтримка на 3560/3750	Є	Є
Статус	Застарілий (deprecated)	Актуальний, рекомендований

На обладнанні Cisco Catalyst 3560 і 3750, яке присутнє у лабораторії, обидва протоколи підтримуються. Саме тому на цих моделях перед командою **switchport mode trunk** необхідно явно вказати тип інкапсуляції:

```
…
MLS(config-if)# switchport trunk encapsulation dot1q
MLS(config-if)# switchport mode trunk
…
```

Без цього команда **switchport mode trunk** поверне помилку, оскільки комутатор не може визначити, який протокол використовувати. На Catalyst 2960 ця команда не потрібна, бо 2960 підтримує виключно dot1q і визначає тип автоматично.

ПеревІРити поточний протокол тегування на trunk-порту можна командою **show interfaces trunk** – у стовпці **Encapsulation** відображається **802.1q** або **isl**.

Сьогодні ISL не використовується у нових розгортаннях. Cisco рекомендує виключно IEEE 802.1Q для всіх trunk-з'єднань.

Native VLAN та нетеговані кадри

Для кожного транкового порту визначається так звана **Native VLAN** (рідна VLAN). Кадри, що належать Native VLAN, передаються через транковий канал у нетегованому вигляді (без вставки тегу 802.1Q). Кадри решти VLAN тегуються відповідним VID.

За замовчуванням на комутаторах Cisco Native VLAN – це VLAN 1. З мІРкувань безпеки рекомендується:

- Змінити Native VLAN з VLAN 1 на будь-яку невикористовувану VLAN (наприклад, VLAN 999);
- Налаштувати тегування кадрів Native VLAN командою **vlan dot1q tag native** (глобально) або **switchport trunk native vlan tag** (на інтерфейсі), щоб запобігти атакам подвійного тегування (double-tagging attack).

Протокол DTP (Dynamic Trunking Protocol)

DTP (Dynamic Trunking Protocol) – фІРмовий протокол Cisco для автоматичного узгодження параметрів транкового з'єднання між двома комутаторами. DTP визначає, чи стане з'єднання транковим, і який протокол тегування буде використовуватись (ISL або 802.1Q).

Режими роботи інтерфейсу щодо DTP:

- **trunk (on)** – примусовий транковий режим; інтерфейс надсилає DTP-кадри та безумовно стає транковим;
- **dynamic desirable** – активно намагається встановити транковий зв'язок, надсилаючи DTP-кадри;
- **dynamic auto** (за замовчуванням) – відповідає на DTP-кадри від сусіда, але сам не ініціює;
- **access** – примусовий режим доступу; DTP-кадри надсилаються, але з'єднання ніколи не стане транковим;
- **nonegotiate** – DTP-кадри не надсилаються і не обробляються; рекомендується поєднувати з режимом **trunk** для підключення до обладнання сторонніх виробників.

Комбінації режимів, за яких формується транковий канал, наведені в таблиці 2.7.

Таблиця 2.7.

Комбінації режимів DTP та результуючий тип з'єднання

Режим	trunk	dynamic desirable	dynamic auto	access
trunk	trunk	trunk	trunk	–
dynamic desirable	trunk	trunk	trunk	access
dynamic auto	trunk	trunk	access	access
access	–	access	access	access

Принцип групування портів (Port-Based VLAN)

При використанні методу групування портів кожен фізичний порт комутатора статично або динамічно прив'язується до певної VLAN. Кадри, отримані на порту доступу, вважаються такими, що належать VLAN, призначеній цьому порту. Порт доступу не додає і не видаляє теги 802.1Q – ця операція виконується виключно всередині комутатора.

Коли комутатор отримує нетегований кадр на порту доступу, він асоціює кадр з VLAN даного порту та пересилає його тільки тим портам, що належать тій самій VLAN (або транковим портам, на яких дана VLAN дозволена). Завдяки цьому трафік різних VLAN є повністю ізольованим на канальному рівні.

Рекомендації Cisco щодо безпеки VLAN

Компанія Cisco розробила перелік базових рекомендацій щодо підвищення рівня захищеності комутованих мереж із VLAN:

1. Відключити всі незадіяні порти та перемістити їх у спеціальну невикористовувану VLAN;
2. Використовувати нестандартну VLAN (відмінну від VLAN 1) як VLAN управління;
3. Не використовувати VLAN 1 для жодного виробничого або адміністративного трафіку;
4. Налаштувати всі порти підключення кінцевих користувачів як порти доступу та вимкнути DTP на цих портах;
5. Явно налаштовувати параметри транкових портів, не покладаючись виключно на DTP;

6. Завжди явно вказувати список дозволених VLAN для транкових каналів;

7. Налаштувати тегування Native VLAN та відкидання нетегованих кадрів на транкових портах;

8. Вимкнути стан порту за замовчуванням – перевести незадіяні порти у shutdown.

Порядок налаштування VLAN на основі групування портів

Порядок налаштування VLAN на основі групування портів на комутаторі Cisco згідно з рекомендаціями виробника:

1. Створити VLAN командою **vlan *vlan-id*** у режимі глобального конфігурування;

2. Вказати текстову назву для VLAN командою **name *text-string*** (необов'язково, але рекомендується для документування);

3. Для інтерфейсу/групи інтерфейсів доступу задати тип access командою **switchport mode access**;

4. Призначити інтерфейс до потрібної VLAN командою **switchport access vlan *vlan-id***;

5. Для транкових інтерфейсів задати тип trunk командою **switchport mode trunk**;

6. Налаштувати параметри транкового каналу (дозволені VLAN, Native VLAN) та вимкнути DTP командою **switchport nonegotiate**;

7. Налаштувати SVI для VLAN управління та призначити IP-адресу комутатору;

8. Вимкнути всі незадіяні порти та перевести їх у спеціальну невикористовувану VLAN.

Основні команди налаштування VLAN

Синтаксис команди **vlan** (режим глобального конфігурування):

vlan *vlan-id*,

де ***vlan-id*** – ідентифікатор (номер) VLAN, може зазначатися в межах від 1 до 4094, для мереж Ethernet типове використання у діапазоні від 2 до 1001.

Синтаксис команди **name** (режим конфігурування VLAN):

name *text-string*,

де ***text-string*** – текстова назва VLAN; якщо текстова назва VLAN явно не зазначається, то система автоматично встановлює назву ви-гляду VLANDDDD, де DDDD – чотирицифровий десятковий номер VLAN.

Синтаксис команди **switchport access vlan** (режим конфігуру-вання інтерфейсу/групи інтерфейсів):

switchport access vlan {*vlan-id* | dynamic},

де ***vlan-id*** – ідентифікатор VLAN;

dynamic – параметр, який зазначає, що належність інтерфей-су/порту до VLAN визначається динамічно (за MAC-адресою), шля-хом запиту до сервера VMPS (VLAN Membership Policy Server).

Синтаксис команди **switchport trunk** (режим конфігурування інтерфейсу/групи):

switchport trunk {allowed vlan *vlan-list* | native vlan *vlan-id* | pruning vlan *vlan-list*},

де **allowed vlan** – службова конструкція, за допомогою якої створюється список дозволених VLAN, для яких транковий інтерфейс може пересилати та отримувати трафік у тегованій формі; за замовчуванням ***vlan-list*** для цієї конструкції дорівнює **all**; ***vlan-list*** у цьому випадку не може дорівнювати **none**;

native vlan – службова конструкція, за допомогою якої створюється список VLAN, для яких транковий інтерфейс може пересилати і отримувати трафік у нетегованій формі;

pruning vlan – службова конструкція, за допомогою якої створюється список VLAN, для яких транковий інтерфейс активований для підтримки режиму VTP-pruning; ***vlan-list*** у цьому випадку не може дорівнювати **all**;

vlan-list – може набувати значень, що наведені нижче; деякі з цих значень доповнюються параметрами ідентифікаторів VLAN IDs:

vlan-atom – список ідентифікаторів VLAN (наприклад, 10-20; 10-30,35-40);

add – додати окрему VLAN або групу VLAN за списком;

all – додати всі VLAN;

except – виключити окрему VLAN або групу VLAN за списком;

none – пустий список;

remove – виключити VLAN зі списку

Синтаксис команди **switchport native** (режим конфігурування інтерфейсу/групи інтерфейсів):

switchport native vlan *vlan-id*,

де ***vlan-id*** – ідентифікатор VLAN.

Налаштування SVI (Switched Virtual Interface) для VLAN управління:

```
…
Switch(config)# interface vlan vlan-id
Switch(config-if)# description text
Switch(config-if)# ip address IP_address network_mask
Switch(config-if)# no shutdown
…
```

Вимкнення DTP на транковому інтерфейсі (рекомендується при підключенні до обладнання сторонніх виробників або при статичному транкуванні):

```
…
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
…
```

Типовий сценарій налаштування VLAN для навчальної мережі

Нижче наведено типовий сценарій налаштування комутаторів з агрегованим транковим каналом:

Створення VLAN

```
…
Switch(config)# vlan 100
Switch(config-vlan)# name DATA-VLAN-A
```

```
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# name DATA-VLAN-B
Switch(config-vlan)# exit
…
```

Агрегований транковий канал

```
Switch(config)# interface range GigabitEthernet0/1-2
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport nonegotiate
Switch(config-if-range)# channel-group 1 mode on
Switch(config-if-range)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100, 200
Switch(config-if)# switchport trunk native vlan 100
Switch(config-if)# exit
…
```

Порівняння Telnet та SSH

Протокол **Telnet** (Teletype Network, RFC 854) – один із найстаріших протоколів для організації інтерактивного термінального доступу до мережних пристроїв. Telnet передає всі дані, у тому числі ім'я користувача та пароль, у відкритому (незашифрованому) вигляді, що робить його вразливим до перехоплення трафіку.

Протокол **SSH** (Secure Shell, RFC 4251–4256) – захищений протокол для організації термінального доступу з криптографічним захистом каналу. SSH забезпечює шифрування всього трафіку між клієнтом і сервером, аутентифікацію та цілісність даних.

Порівняння протоколів Telnet та SSH наведено в таблиці 2.8.

Таблиця 2.8.

Порівняння протоколів Telnet та SSH

Характеристика	Telnet	SSH
Шифрування трафіку	Відкритий текст	AES, 3DES тощо
Порт	TCP 23	TCP 22
Аутентифікація	Відкритий пароль	Захищений пароль або ключ
Цілісність даних	ПеревІРка відсутня	HMAC
Підтримка PKI	Відсутня	RSA-ключі
Рекомендація до застосування	У лабораторних умовах	У виробничих мережах

Версії SSH

Існують дві версії протоколу SSH:

- **SSH версії 1 (SSHv1)** – перша реалізація; містить відомі вразливості (Man-in-the-Middle атака) і вважається застарілою. На обладнанні Cisco рекомендується відключити SSHv1.

- **SSH версії 2 (SSHv2)** – сучасна версія з покращеним шифруванням, обміном ключами Diffie-Hellman та строгою перевIPкою цілісності. Cisco рекомендує використовувати виключно SSHv2.

Налаштування SSH на комутаторах Cisco

Для налаштування SSH-доступу на комутаторах Cisco необхідно виконати такий порядок дій:

1. Задати доменне ім'я пристрою (обов'язково для генерації RSA-ключа);
2. Задати ім'я хосту (**hostname**) – воно використовується у RSA-ключі;
3. Створити локальних користувачів командою **username**;
4. Згенерувати пару RSA-ключів командою **crypto key generate rsa**;
5. Обмежити версію SSH (рекомендується SSHv2) командою **ip ssh version 2**;
6. Налаштувати лінії VTY для використання SSH командами **transport input ssh** та **login local**.

Для підключення по SSH з робочої станції (що знаходиться у VLAN управління та має IP-адресу з тієї ж підмережі) використовуються такі команди:

З командного рядка Windows:

C:\> ssh -l Admin 192.168.1.2

де **Admin** – ім'я користувача, **192.168.1.2** – IP-адреса VLAN управління комутатора.

З терміналу Linux:

$ ssh Admin@192.168.1.2

З PuTTY:

у полі **Host Name** вказати IP-адресу комутатора, обрати **Connection type** – SSH, **Port** – 22, натиснути Open. У вікні терміналу ввести ім'я користувача та пароль.

З іншого пристрою Cisco (маршрутизатора або комутатора):

Router# ssh -v 2 -l Admin 192.168.1.2

Команди моніторингу та діагностики VLAN на комутаторах Cisco

Для моніторингу та діагностики VLAN на комутаторах Cisco застосовуються спеціалізовані та загальні команди show (таблиця 2.9).

Таблиця 2.9.

Команди діагностики VLAN та SSH на комутаторах Cisco

Команда	Призначення
show vlan	Повна інформація про всі VLAN та їх порти
show vlan brief	Скорочений перегляд: номер, назва, стан, порти
show vlan id *vlan-id*	Детальна інформація про конкретну VLAN за номером
show vlan name *vlan-name*	Інформація про VLAN за її назвою
show vlan summary	Зведена інформація: кількість VLAN, VTP VLAN тощо
show interfaces switchport	Параметри VLAN для всіх інтерфейсів
show interfaces *interface-type interface-id* switchport	Параметри VLAN для конкретного інтерфейсу

Команда	Призначення
show interfaces trunk	Параметри транкових з'єднань та дозволені VLAN
show interfaces vlan *vlan-id*	Стан та статистика SVI-інтерфейсу VLAN
show dtp	Параметри DTP для всього комутатора
show dtp interface *interface-type interface-id*	Параметри DTP для конкретного транкового порту
show running-config	Поточна конфігурація пристрою (містить налаштування VLAN)
show mac-address-table	Таблиця MAC-адрес комутатора з VLAN
show ip ssh	Версія та параметри SSH-сервера
show users	Активні сесії на пристрої (у т.ч. SSH-сесії)

Комбінування VLAN з агрегованим каналом EtherChannel

Перевагами реалізації двох технологій агрегування та транкування каналу 802.1Q:

- Збільшена **пропускна здатність** між комутаторами (2×1 Гбіт/с = 2 Гбіт/с при двох фізичних каналах);
- **Відмовостійкість**: при виході з ладу одного з фізичних каналів EtherChannel логічний канал залишається активним, а трафік усіх VLAN продовжує передаватися;
- **Єдина точка управління**: транкові параметри (дозволені VLAN, Native VLAN) налаштовуються на логічному інтерфейсі port-channel, а не на кожному фізичному інтерфейсі окремо;
- **STP** (Spanning Tree Protocol) сприймає EtherChannel як єдиний логічний канал, що спрощує топологію дерева та прискорює збіжність.

Важливою особливістю є порядок налаштування: параметри інтерфейсу VLAN (**switchport mode trunk**, **switchport trunk allowed vlan**) необхідно задавати саме на логічному інтерфейсі **port-channel**, а не на фізичних інтерфейсах, що входять до групи. Фізичні інтерфейси мають наслідувати параметри логічного port-channel-інтерфейсу автоматично.

ПеревІРити стан агрегованого транкового каналу можна командами:

- **show etherchannel summary** – стан EtherChannel та фізичних членів групи;
- **show interfaces port-channel *port-channel-id* switchport** – параметри транкування логічного каналу;
- **show interfaces trunk** – відображення port-channel у переліку транкових з'єднань.

Рекомендована послідовність перевІРки роботи VLAN і транків 802.1Q

Рекомендована послідовність перевІРки після завершення налаштування наведена нижче. Для кожної команди показано характерний вивід та пояснення ключових полів.

1. ПеревІРка створених VLAN та призначення портів.

```
Switch# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
10   STUDENTS                         active    Fa0/1, Fa0/2
20   TEACHERS                         active    Fa0/3, Fa0/4
100  MANAGEMENT                       active
```

У таблиці повинні бути присутні всі створені VLAN зі статусом **active**. У стовпці Ports перелічені access-порти, призначені до кожної VLAN. Trunk-порти **не відображаються** у виводі цієї команди – для них використовуйте show interfaces trunk. VLAN 100 без портів – нормально для management-VLAN, доступ до якої здійснюється лише через транк.

2. ПеревІРка стану trunk-каналу.

```
Switch# show interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/24      on               802.1q         trunking      100
ort        Vlans allowed on trunk
Fa0/24      1,10,20,100
Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,100
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,100
```

Status повинен бути **trunking** – порт активно передає тегований трафік. Encapsulation – **802.1q**. Native VLAN – повинна збігатися на обох сторонах транка (тут – 100). У рядку «Vlans allowed and active» – VLAN, які реально активні на цьому транку. Якщо VLAN не у переліку «allowed» – кадри цієї VLAN через транк не передаються.

3. ПеревІРка стану конкретного порту.

```
Switch# show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (STUDENTS)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Administrative Mode – те, що задано адміністратором; Operational Mode – фактичний режим. Для access-порту обидва повинні бути «static access». Поле Access Mode VLAN – VLAN, до якої призначений порт. Якщо Operational Mode = «trunk» замість заданого «access» – це означає, що порт перейшов у trunk-режим автоматично через DTP – небезпечна ситуація, потрібна команда **switchport nonegotiate**.

4. ПеревІРка таблиці MAC-адрес.

```
Switch# show mac address-table
          Mac Address Table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0050.ab12.3456    DYNAMIC     Fa0/1
  10    0050.ab12.3478    DYNAMIC     Fa0/24
  20    0050.ab12.3490    DYNAMIC     Fa0/3
 100    0050.ab56.7800    DYNAMIC     Fa0/24
```

Таблиця MAC-адрес показує, які пристрої комутатор бачить на кожному порту і у якій VLAN. MAC-адреси, отримані через trunk-порт (Fa0/24), належать кінцевим пристроям з іншого комутатора. Якщо MAC-адреса з'явилася не у тій VLAN – помилка призначення порту. Якщо MAC-адреси з access-порту немає у таблиці – пристрій не передає трафік або відключений.

5. ПеревІРка зв'язку між пристроями.

```
C:\> ping 192.168.10.20
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128

C:\> ping 192.168.20.20
Request timed out.
```

У межах однієї VLAN (наприклад, VLAN 10) пристрої повинні бачити один одного через ping. У межах різних VLAN ping без маршрутизатора або L3-комутатора **не повинен працювати** – це і є сегментація. Якщо ping між VLAN несподівано працює – VLAN не ізольовані (ймовІРно, обидва порти в одній VLAN, або є нелегальний шлюз).

Типові помилки при налагодженні VLAN і транків 802.1Q

1. **VLAN не створений у базі даних комутатора.** Просте призначення команди **switchport access vlan *vlan-id*** без попереднього створення VLAN у глобальній конфігурації призводить до того, що порт залишається у стандартній VLAN 1 або переходить у inactive-стан. Перед призначенням порту до VLAN необхідно створити її командою **vlan *vlan-id*** у режимі глобальної конфігурації. ПеревІРяти командою **show vlan brief** – VLAN повинна мати статус **active**.

2. **Порт залишений у режимі dynamic auto/desirable у production-мережі.** За замовчуванням Cisco-комутатори увімкнені в режимі **dynamic auto** , що дозволяє порту автоматично перейти у trunk при отриманні DTP-кадрів. Це створює загрозу безпеки (VLAN hopping). У production-мережі обов'язково задавати режим явно: **switchport mode access** для портів кінцевих пристроїв або **switchport mode trunk** для транків. На access-портах додатково вимикати DTP командою **switchport nonegotiate**.

3. **Розбіжність Native VLAN на trunk-каналі.** Native VLAN – це VLAN, кадри якої передаються транком БЕЗ тегування. Якщо на двох сторонах транка налагоджено різні Native VLAN – комутатор Cisco видає попередження «native VLAN mismatch detected» і кадри Native VLAN не доходять до іншого боку. Обов'язково встановлювати однакову Native VLAN на обох сторонах командою **switchport trunk native vlan *vlan-id***. Рекомендується змінити Native VLAN з дефолтної 1 на іншу (наприклад, виділену management-VLAN) – для безпеки.

4. **VLAN не дозволена на транку.** За замовчуванням транк передає всі VLAN (1–4094). Однак якщо адміністратор обмежив список командою **switchport trunk allowed vlan *vlan-list***, то всі інші VLAN автоматично заборонені. Помилка – забути додати нову VLAN до allowed-списку. ПеревІРяти командою **show interfaces trunk** – у стовпці «Vlans allowed and active in management domain» повинні бути всі необхідні VLAN. Для додавання нової VLAN до існуючого списку використовувати **switchport trunk allowed vlan add *vlan-id***.

5. **Помилкова інкапсуляція на транку.** Деякі моделі Cisco-комутаторів (наприклад, серії 3560) підтримують дві технології транкінгу: 802.1Q і ISL (фІРмовий, застарілий). За замовчуванням може бути встановлено dynamic-режим інкапсуляції, що призводить до неузгодженості. Обов'язково задавати явно командою **switchport trunk encapsulation dot1q** перед командою switchport mode trunk. На моделях, що підтримують лише 802.1Q (наприклад, 2960), ця команда недоступна – інкапсуляція встановлюється автоматично.

6. **Management VLAN не налагоджена або без шлюзу.** Для віддаленого керування комутатором використовується SVI (інтерфейс VLAN). Помилки: SVI створено, але не введено в експлуатацію командою **no shutdown**; SVI має IP-адресу, але порт-член Management-VLAN не існує (немає трафіку для активації SVI); не задано шлюз за замовчуванням командою **ip default-gateway**, що унеможливлює керування з іншої підмережі. ПеревІРяти командою **show ip interface brief** – SVI повинен мати стан up/up.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке VLAN? Яке призначення та основні переваги технології VLAN у комутованих мережах?
2. Поняття широкомовного домену. Яким чином VLAN обмежує розмIP широкомовного домену?
3. Які методи ідентифікації VLAN існують? Охарактеризуйте метод групування портів (port-based VLAN).
4. Що таке порт доступу (access port)? Чим він відрізняється від транкового порту (trunk port)?
5. Що таке транковий канал? Яке його призначення у мережі з декількома VLAN?
6. Охарактеризуйте стандарт IEEE 802.1Q. Яка структура тегованого кадру 802.1Q?
7. Скільки VLAN можна ідентифікувати за допомогою поля VID у тегу 802.1Q? Поясніть з урахуванням розмIPу поля у бітах.
8. Що таке Native VLAN? Як передаються кадри Native VLAN через транковий канал? Яка VLAN є Native за замовчуванням на комутаторах Cisco?
9. Що таке атака подвійного тегування (double-tagging attack)? Яким чином налаштування Native VLAN допомагає її запобігти?
10. Що таке протокол DTP (Dynamic Trunking Protocol)? Які режими роботи він підтримує? При яких комбінаціях режимів формується транковий канал?
11. Що таке VLAN управління (Management VLAN)? Яке її призначення? Чому не рекомендується використовувати VLAN 1 як VLAN управління?
12. Що таке SVI (Switched Virtual Interface)? Яке призначення цього інтерфейсу? Якою командою він налаштовується?
13. Чи можуть хости різних VLAN взаємодіяти між собою без маршрутизатора або L3-комутатора? Поясніть відповідь.
14. Перелічіть основні рекомендації Cisco щодо підвищення рівня захищеності VLAN. Поясніть призначення кожного заходу.
15. Яким чином вимикається протокол DTP на транковому порту? Коли це доцільно застосовувати?
16. Які основні команди налаштування VLAN на основі групування портів та транкових каналів існують на комутаторах Cisco? Поясніть синтаксис кожної команди.
17. Яким чином агрегований канал EtherChannel поєднується з транковим каналом 802.1Q? На якому інтерфейсі (фізичному чи логічному port-channel) налаштовуються параметри VLAN і чому?